Subject: **INFORMATION TECHNOLOGY DISASTER RECOVERY AND BUSINESS CONTINUITY POLICY**

Purpose:

The purpose of this policy is to ensure that information technology (IT) resource investments made by the County are protected against service interruptions, including large scale disasters, by the development, implementation, and testing of a Disaster Recovery / Business Continuity (DR/BC) plan.

Policy:

1. POLICY

1.1. *Overview:* Every organization is at risk from potential disasters – accidental, natural, commercial or willful – that may include:

- Environmental issues such as severe weather, electricity outages, fire, water from leaking roofs or pipes
- Mechanical failures such as hard disk and tape drive failures and computer outages
- External attacks by hackers, vandals, saboteurs, or disgruntled persons who want to disrupt IT operations
- Malware, such as viruses, worms, and Trojan horses
- Software errors
- Procedural or user errors

When unexpected events happen that affect the County's IT services, there must be plans and procedures in place that allow for business operations to resume. A completed DR/BC Plan is a formal document that includes clear roles, responsibilities, business priorities and specific tasks to manage a disruption and is available for reference before, during, and after an event has occurred.

This policy and the DR/BC Plan will help minimize the impact of a disaster by:

- Taking the necessary steps to prepare for a disaster
- Recognizing failures and breakdowns when they occur
- Ensuring that critical data is properly backed up and stored
- Keeping the business operating during the period of the disaster

This policy defines the IT Disaster Recovery and Business Continuity strategy requirements to run critical business applications and the associated processes to transition smoothly in the event of a disaster.

1.2. *Recovery Objectives:* Two key recovery objectives include the recovery time objective and the recovery point objective.

1.2.1. Recovery Time Objective (RTO) - RTO defines how quickly you need to restore applications and have them fully functional again. The faster your RTO requirement, the closer you move to zero interruption in uptime and the highest availability requirements. The RTO is the time objective to bring a system back online following a failure.

1.2.2. Recovery Point Objective (RPO) - RPO defines the point at which the business absolutely cannot afford to lose data. It points to a place in each data stream where information must be available to put the application or system back in operation. The RPO is the acceptable amount of data loss since the last good backup prior to the point of failure. Again, the closer you come to zero data loss and continuous real-time access, the higher availability you will require.

An IT Business Impact Analysis survey will be done periodically to determine the effect of an interruption of IT services on each business unit and the organization as a whole in the event of a disaster. The Business impact Analysis survey will be used to help prioritize the applications and technology services required in the event of a disaster.

Achieving the highest level of availability with minimal data loss is the goal (RTO and RPO close to zero).

1.3. *Requirements for Disaster Recovery:* Three main requirements for disaster recovery include:

- Minimize risk
- Minimize downtime
- Control Cost

To meet these requirements while allowing for business continuity for critical applications, a form of data replication and server virtualization is required.

Data replication is the process of copying information so as to ensure consistency between redundant resources (such as software or hardware components) to improve reliability, fault-tolerance, or accessibility. The same data is copied onto storage devices at a remote location (or disaster recovery site) via normal network connectivity.

Virtualization software allows recovery from server failures by automatically restarting virtual machines on alternate servers located at a remote location (or disaster recovery site). Server virtualization makes high availability and disaster recovery more straightforward and cost effective.

Virtualization, used with data replication on a storage area network, addresses the recovery objective to achieve the highest level of availability with minimal data loss.

The disaster recovery site requires:

- High-speed connectivity to the County's wide area network (WAN)
- A backup generator to provide all electrical requirements to the data centre room in case of electrical outage
- Sufficient heating / cooling to provide the proper operating and storage environment for the equipment

If, during an emergency, the primary site is not available, the technology at the disaster recovery site is automatically utilized.

1.4. *Test DR/BC Plan:* It is essential that the DR/BC plan be thoroughly tested and evaluated on a regular basis (at least annually). Procedures to test the plan should be documented. The tests will provide the organization with the assurance that all necessary steps are included in the plan. Other reasons for testing include:

- Determining the feasibility and compatibility of backup facilities and procedures
- Verifying the effectiveness of the recovery method
- Establishing if the recovery objectives are achievable
- Identifying areas in the plan that need modification or clarification
- Providing training to the team managers and team members
- Demonstrating the ability of the organization to recover
- Providing motivation for maintaining and updating the DR/BC Plan
- Identifying improvements required to the Plan

1.5. *Train Employees to Execute the DR/BC Plan:* Training will consist of:

- Making employees aware of the need for a DR/BC plan.
- Informing all employees of the existence of the plan and providing procedures to follow in the event of an emergency
- Training all personnel with responsibilities identified in the plan (and their alternates) to perform the DR/BC procedures
- Providing the opportunity for recovery teams to practice DR/BC skills

2. DEFINITIONS

2.1 *Business Continuity*: is the uninterrupted availability of all key information technology resources supporting essential business functions.

2.2 *Business Continuity Plan:* A collection of procedures and information that is developed, compiled, and maintained in readiness for use in the event of an emergency or disaster.

2.3 *Business Continuity Planning (BCP)* is used to create and validate a practiced plan for how an organization will recover and restore partially or completely interrupted critical function(s) within a predetermined time after a disaster or extended disruption. This goes beyond the enterprise computers, networks and data bases. Disaster Recovery Planning and/or Business Continuity Planning facilitate how a company will keep functioning after a disruptive event until its normal facilities are restored.

2.4 *Disaster:* Any loss of utility service (power, water), connectivity (system sites), or catastrophic event (accidental, natural, commercial or willful) that causes an interruption to Haldimand County's information technology (IT) resource investments.

2.5 *Disaster Recovery:* is the process of regaining access to the data, hardware and software necessary to resume critical business operations after a natural or a human caused disaster.

2.6 *Disaster Recovery Planning (DRP)* is the process by which you resume business after a disruptive event. This typically means that you can get the identified enterprise computers, networks, and databases operational.

3. RESPONSIBILITIES

3.1 *Information Systems Division:* The I.S. Division is responsible to ensure regular testing of the DR/BC Plan is completed.

3.2 *Manager of Information Systems:* The I.S. Manager is responsible to ensure the DR/BC Plan is updated as required. The I.S. Manager is also responsible to ensure I.S. Divisional staff are trained to execute the DR/BC Plan.

3.3 *Business Units:* Divisional Managers and/or Supervisors are responsible to fill out an IT Business Impact Analysis survey annually (when business specific applications are deployed or when business practices change) to help determine and identify the effect of an interruption of IT services on each business unit and the organization as a whole. The survey will be used to prioritize the applications and technology services and timelines required in the event of a disaster.

4. REFERENCES

4.1. Haldimand County Disaster Recovery / Business Continuity Plan

4.2. Haldimand County Backup and Data Recovery Policy

Topical Index	Corporate Services
Policy Number	2009-03
Short Title	Information Technology Disaster Recovery and Business Continuity
SMT Approval Date	September 2, 2009
Council in Committee	October 26, 2009 Recommendation # 28
Council Approval Date	November 2, 2009 Resolution # 306-09
Originating Department	CS-IS-02-2009 and CS-IS-03-2009 (Supplementary)
Revisions	

PURPOSE

The purpose of this IT Disaster Recovery and Business Continuity (DR/BC) Plan is to prepare Haldimand County for the effect of extended technology service outages caused by factors beyond our control (e.g., natural disasters, man-made events), and to restore services to the optimal extent possible in a minimum time frame. Preventive measures are expected to be implemented whenever possible to minimize network failure and to recover as rapidly as possible when a failure occurs.

SCOPE, GOALS AND OBJECTIVES

The **scope** of this Business Continuity Plan (BCP) is for Haldimand County to establish the capability to respond to major disruptive events with minimal impact to the County's staff.

The **goals** of the DR/BC Plan are to:

- Build the County's technology resources' resilience and capacity to manage through any major disruptions
- Promptly and effectively respond to emergencies and disasters affecting the County's technology resources
- Mitigate the impact of loss to physical assets and information systems
- Maintain the integrity and quality of the DR/BC Plan through regular reviews, updates, simulation exercises and systems assessments
- Promote County-wide awareness about the importance and purpose of IT business continuity.

The **objectives** of the DR/BC Plan are to effectively manage the resumption of critical technology services resulting from a major disruptive event within established recovery time objectives (RTOs) and recovery point objectives (RPOs). The RTOs and RPOs established for Haldimand County applications and core IT services are outlined in the section entitled "Summary of Critical Services (with recovery objectives and recovery priorities)".

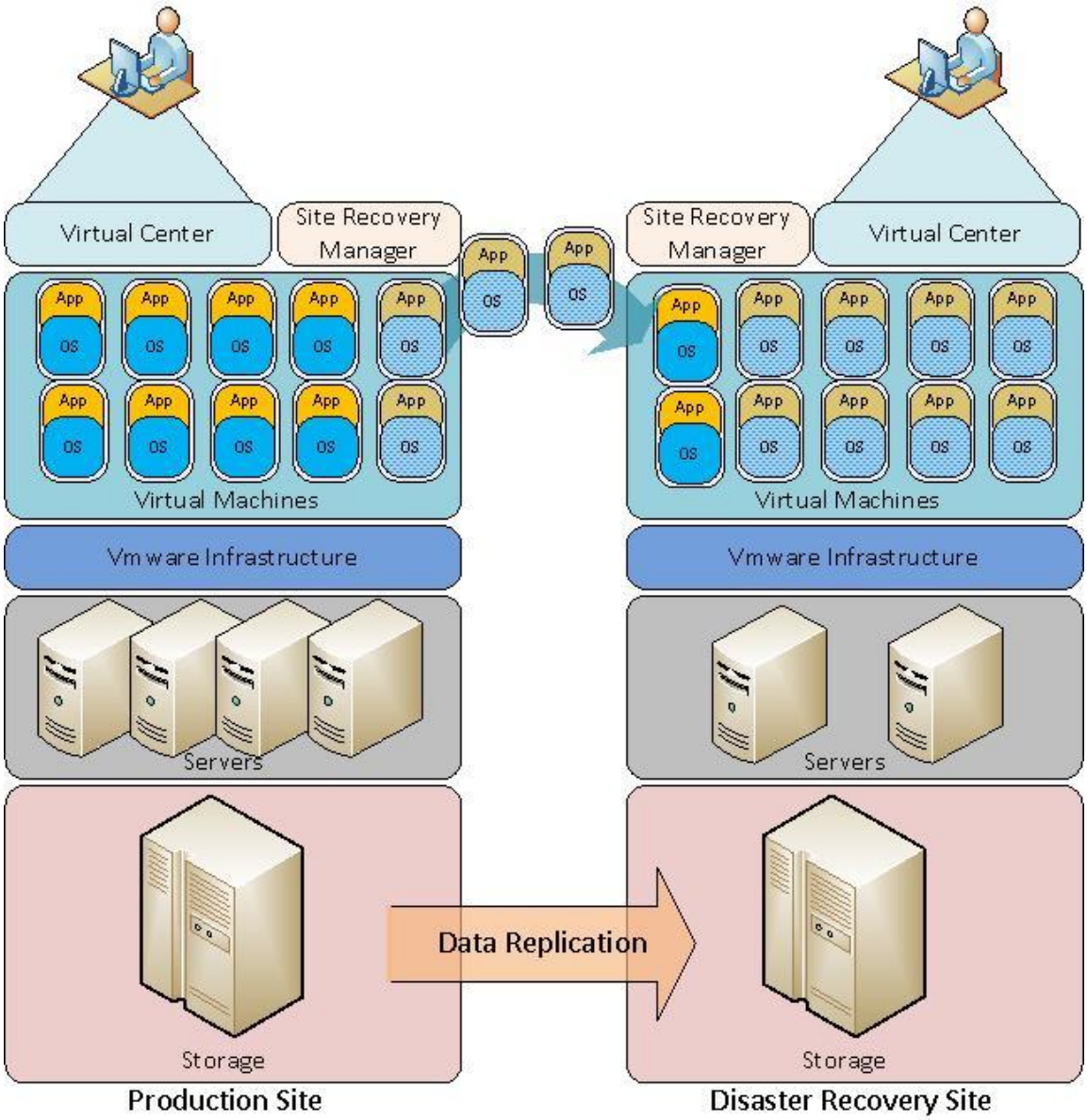
STRATEGY

This DR/BC Plan addresses the scenario of complete loss of the County's main data center. The set up of a second remote site with data replication and server virtualization is crucial to allow for IT business continuity. Current technologies – storage consolidation via a storage area network (SAN) and virtualization – have options available for a cost-effective, highly available solution for disaster recovery.

Server virtualization makes high availability and disaster recovery more straightforward and cost effective than with past technology. Without requiring any application level programming, virtualization software can recover from server failures by automatically restarting virtual machines on alternate servers, making practically any application highly available. If disaster takes an entire geographic location out of service, virtualization

allows virtual machines to be restarted at an alternate site from remote copies of their logical volumes. Unlike the painstaking setup required with physical servers, virtual machines can be started at the remote site easily and quickly. Virtualization used with data replication on a storage area network addresses the recovery objective to achieve the highest level of availability with minimal data loss.

The following visually depicts the strategy with the “Production Site” and “Disaster Recovery Site”. As depicted in the picture below, when a virtual machine goes “down” at the production site, another virtual machine at the disaster recovery site automatically starts or “takes over”. This, along with data being replicated at the disaster recovery site, gives a high availability solution for disaster recovery and business continuity.



KEY ROLES AND RESPONSIBILITIES

With server virtualization and data replication, the disaster recovery setup is simplified. Software tools are used to deliver advanced disaster recovery management and automation. Site recovery software will simplify and automate the recovery workflows, turn manual recovery run-books into automated recovery plans, and provide central management of recovery plans.

As part of their day to day duties, I.S. staff will ensure the virtualization and data replication software and hardware is configured to allow for automated disaster recovery.

The I.S. Network Support Analysts and the Systems Support staff will:

- Build recovery processes in advance
- Create, test, update and execute recovery plans
- Automate testing of recovery plans
- Automate execution of recovery process
- Allocate and manage recovery resources
- Monitor and make adjustments as needed.

Information Systems Division Staff member responsibilities include:

- Keeping an updated contact list of their work team members' work, home, and cell phone numbers both at home and at work
- Keeping a printed copy of this plan and related policies and procedures at home in case the disaster happens after normal work hours. All team members should familiarize themselves with the contents of this plan.

The Manager of Information Systems is responsible to:

- Ensure the DR/BC Plan is updated as required
- Ensure I.S. Divisional staff are trained to execute the DR/BC Plan.

SUMMARY OF APPLICATIONS AND IT CORE SERVICES (WITH RECOVERY OBJECTIVES)

A summary of the applications and IT core services, their recommended maximum down time and maximum data loss, are listed in the following table:

Application Name	Maximum Down Time	Maximum Data Loss
Dominion Voting (Elections Software) ** only during election time	Up to 4 hrs	Zero
Responder 4000 (Nurse Call system at Grandview)	Up to 4 hrs	Up to 24 hrs
AutoScale – waste disposal / scale software	Up to 24 hrs	Up to 24 hrs
CityView – Building & By-Law (permitting, inspections, by-law enforcement)	Up to 24 hrs	Up to 24 hrs
CityView – Planning & Development	Up to 24 hrs	Up to 24 hrs
CityView – Property Management	Up to 24 hrs	Up to 24 hrs
CLASS – Leisure Link (on-line registration)	Up to 24 hrs	Up to 24 hrs
CLASS – Leisure Recreation Program and Facility Registration	Up to 24 hrs	Up to 24 hrs
CompuCare (Grandview's resident trust accounts)	Up to 3 days	Up to 24 hrs
Corporate Website (www.haldimandcounty.on.ca)	Up to 24 hrs	Up to 24 hrs

Application Name	Maximum Down Time	Maximum Data Loss
Grey Island InterFleet - Global Positioning System/Automated Vehicle Location (EMS)	Up to 24 hrs	Up to 24 hrs
Horizon – Library Automation (circulation)	Up to 24 hrs	Up to 24 hrs
ICON – POA system	Up to 24 hrs	N/A
Liberty Court Recording System – POA	Up to 24 hrs	Zero
MEDeCare – Grandview's patient care system	Up to 24 hrs	Up to 24 hrs
MOH ADDAS (EMS)	Up to 24 hrs	N/A
StarGarden – Human Resource Management System for payroll, employee benefits, health and safety	Up to 24 hrs	Up to 24 hrs
Sysco Synergy – Dietary software (Grandview)	Up to 24 hrs	Up to 24 hrs
Vailtech – Financial System (general ledger)	Up to 24 hrs	Up to 24 hrs
Vailtech – Financial System (accounts payable)	Up to 24 hrs	Up to 24 hrs
Vailtech – Financial System (accounts receivable)	Up to 24 hrs	Up to 24 hrs
Vailtech – Financial System (tax billing & collection)	Up to 24 hrs	Up to 24 hrs
WorkTech – Infrastructure Asset Management and Work Management	Up to 24 hrs	Up to 24 hrs
Financial Manager's Workbench (FMW) – Budget planning and reporting	Up to 3 days	Up to 24 hrs
GIS applications – AutoDesk / ESRI software	Up to 3 days	Up to 24 hrs
GIS – on-line	Up to 3 days	N/A
Horizon Information Portal (on-line catalog)	Up to 3 days	Up to 24 hrs
IDT – Grandview's scheduling software	Up to 3 days	Up to 24 hrs
ProFuel – fuel (gas / diesel) control software (Fleet)	Up to 3 days	Up to 24 hrs
ProFuel – liquid (water) control software used by water depots	Up to 3 days	Up to 24 hrs
Staff Information Network (intranet)	Up to 3 days	Up to 1 week
ACRPlus – ambulance call tracking	Up to 1 week	Up to 24 hrs
Alarm systems software (Facilities)	Up to 1 week	Up to 1 week
Aqua Cad® Suite (W&WW)	Up to 1 week	N/A
CityView – Vital Statistics (birth / death registrations)	Up to 1 week	Up to 24 hrs
CompuSpread – salt spreader s/w (Roads Operations)	Up to 1 month	Up to 24 hrs
Corporate Reporting including Crystal Reports	Up to 1 week	Up to 1 week
EPI Suite (photo ID)	Up to 1 week	Up to 1 week
Fleetguard Master Catalog (fleet diagnostic software)	Up to 1 week	N/A
FitPro – respirator fit testing	Up to 1 week	Up to 1 week
HeartStart Event Review Suite (Defibrillator software - EMS)	Up to 1 week	Up to 1 week
MOH Locator (EMS)	Up to 1 week	Up to 24 hrs
NetLoan – administration of public access computers at Library Branches	Up to 1 week	Up to 1 week
OrgPlus – Organizational Charting	Up to 1 month	N/A
SIC200 – Insurance database (Support Services)	Up to 1 week	Up to 1 week
Stone Orchard – Cemetery software	Up to 1 week	Up to 24 hrs

Core IT Services	Maximum Down Time	Maximum Data Loss
Symantec Endpoint Protection (Antivirus)	Zero	N/A
BlackBerry Services	Up to 4 hrs	N/A
Outlook (Microsoft Exchange)	Up to 4 hrs	Up to 24 hrs
Telephone / Long distance service	Up to 4 hrs	N/A
Access to local service (HelpDesk)	Up to 24 hrs	N/A
Access to network drive H: (personal)	Up to 24 hrs	Up to 24 hrs
Access to network drive S: (shared forms / templates)	Up to 24 hrs	Up to 24 hrs
Access to network drive T: (departmental / divisional)	Up to 24 hrs	Up to 24 hrs
Automated Attendant	Up to 24 hrs	N/A
Internet Access	Up to 24 hrs	N/A
Symantec Backup	Up to 24 hrs	N/A
Total Traffic Control (web content control / spam filtering)	Up to 24 hrs	Up to 1 week
Voice Mail	Up to 24 hrs	Up to 24 hrs
Citrix	Up to 3 days	N/A
Citrix Remote Access	Up to 3 days	N/A
Inbound 800 Service (Tourism)	Up to 3 days	N/A
Network Monitoring	Up to 3 days	N/A
Network Printing	Up to 3 days	N/A
Outlook Web Access	Up to 3 days	N/A
ActiveScout (intrusion detection and prevention)	Up to 1 week	N/A
Library Wireless Networks	Up to 1 week	N/A
Microsoft Windows Server Update Services	Up to 1 week	N/A
Network Scanning	Up to 1 week	N/A
SpiceWorks (IT Helpdesk Software)	Up to 1 week	Up to 24 hrs

Applications and core IT services with a maximum down time of 24 hours or less are considered to be critical.

TESTING THE DISASTER RECOVERY / BUSINESS CONTINUITY PLAN

The DR/BC plan shall be tested on, at least, an annual basis. Any change in the infrastructure that affects the disaster recovery strategy will also trigger a test of the DR/BC plan. The test may be in the form of a walk-through, mock disaster or component testing.

There are several key objectives of a test of which the main ones are:

- exercise the recovery processes and procedures
- familiarize staff with the recovery process and documentation
- verify the effectiveness of the recovery documentation
- verify the effectiveness of the recovery site
- establish if the recovery objectives are achievable
- identify improvements required to the DR strategy, infrastructure, and recovery processes

PLAN REVIEW AND MAINTENANCE

This plan is intended to be a living document and as such must be reviewed on a regular basis. The plan will be reviewed semi-annually and exercised on an annual basis.

The plan will be stored in a common location where it can be viewed by system site personnel and the I.S. Division Team. Hard copies of the plan will be provided to all I.S. Division staff.

Data Replication using Storage Area Networks (SANs)

The Storage Area Network (SAN) device was developed as a common place for a network to store and protect its data. With the SAN, all of the physical disks are co-located in a common disk array. This allows the business to consolidate the data in one place while allowing all of the servers to connect to the data storage from anywhere within the network.

The growth of files, e-mail, databases, and application data drives a constant need for more storage. By consolidating storage resources onto a SAN you can:

- centralize storage and reduce administrative overhead
- simplify IT operations and reduce total IT expenditures
- expand storage capacity, performance, and network bandwidth online without downtime
- increase availability and protect critical data sets
- consolidate storage assets across multiple OS environments.

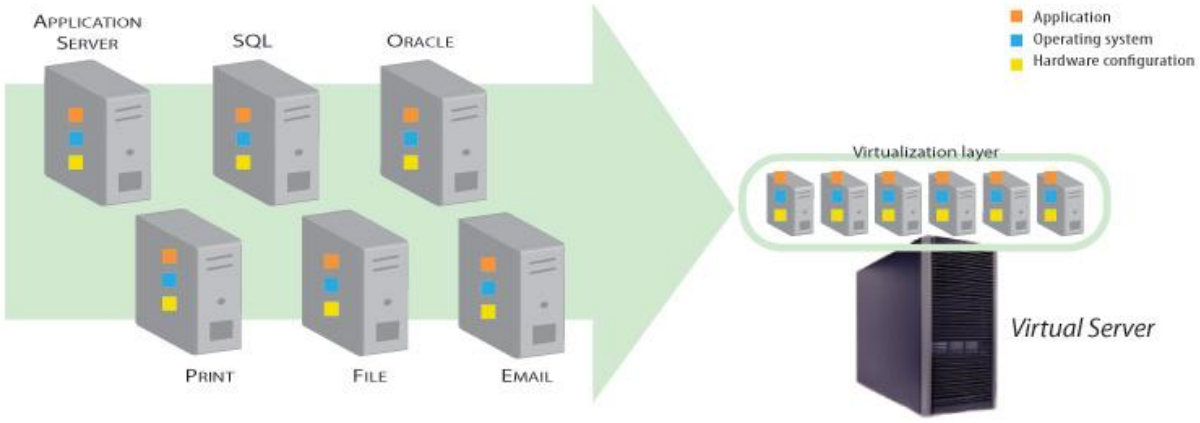
Two SANs will allow for data replication between a production site and a disaster recovery site. Replication is the process of copying information so as to ensure consistency between redundant resources, such as software or hardware components, and to improve reliability, fault-tolerance, or accessibility. The same data is copied onto storage devices at a remote location (or disaster recovery site) via normal network connectivity. The data stored on the existing SAN at the production site would be replicated to a SAN installed at the disaster recovery site.

Server Virtualization

PC Magazine's encyclopedia definition of hardware virtualization is: *Partitioning the computer's memory into separate and isolated "virtual machines" which simulates multiple machines within one physical computer. It enables multiple copies of the same or different operating systems to run in the computer and also prevents applications from interfering with each other.*

Virtualization is a technology that allows you to transform hardware into software. Virtualization allows you to run multiple operating systems simultaneously on a single computer. Each copy of an operating system is installed onto a virtual machine.

The graphic below visually depicts multiple fileservers “virtualized” onto one physical server:



Implementing additional virtual servers at the primary site, as well as the remote disaster recovery site, will allow for business continuity in the event of a disaster. Additional components of the virtualization software, VMware, have built-in continuous availability that, in the event of a server failure, affected virtual machines are automatically restarted on other physical servers in the VMware infrastructure resource pool that have spare capacity.